

Date: Aug 21 2020

United States District Court
NORTHERN DISTRICT OF GEORGIA

JAMES N. HATTEN, Clerk

By: B. Evans
Deputy Clerk

UNITED STATES OF AMERICA

v.

CRIMINAL COMPLAINT

Aleksandr Vladimirovich Spitsyn

Case Number: 1:20-MJ-684

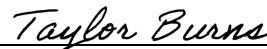
I, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief. From in or about May 2018 and continuing today in the Northern District of Georgia and elsewhere, the defendant did, conspire to commit money laundering, to wit, the defendant conspired to knowingly conduct or try to conduct a financial transaction, knowing that the money or property involved in the transaction were the proceeds of some kind of unlawful activity, that the money or property did come from an unlawful activity, specifically wire or bank fraud; and the defendant knew that the transaction was designed, in whole or in part, to conceal or disguise the nature, location, source, ownership, or the control of the proceeds,

in violation of Title 18, United States Code, Section(s) 1956(h).

I further state that I am a(n) Special Agent with the Federal Bureau of Investigation (FBI) and that this complaint is based on the following facts:

PLEASE SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof. Yes



Signature of Complainant
Taylor Burns

Based upon this complaint, this Court finds that there is probable cause to believe that an offense has been committed and that the defendant has committed it. Sworn to before me, and subscribed in my presence

August 21, 2020

Date

at Atlanta, Georgia

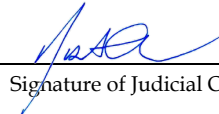
City and State

JUSTIN S. ANAND

UNITED STATES MAGISTRATE JUDGE

Name and Title of Judicial Officer

AUSA Thomas J. Krepp / 2015R00910



Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Taylor Burns, a Special Agent with the Federal Bureau of Investigation (FBI), being first duly sworn, depose and state under oath as follows:

INTRODUCTION

1. This Affidavit is made in support of a criminal complaint for ALEKSANDR VLADIMIROVICH SPITSYN ("SPITSYN") for violations of Title 18, United States Code, Section 1956(h) (money laundering conspiracy).

AFFIANT BACKGROUND

2. I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed by the FBI since March 2016. I am currently assigned to the Atlanta Field Office. As a Special Agent, I am authorized to investigate a wide variety of crimes involving violations of federal law. I have received extensive training as a Special Agent at the Federal Bureau of Investigation Academy in Quantico, Virginia. I have completed outside training and college courses in computer programming, networking, and information security. Before I was

employed by the FBI, I was a desktop support manager with industry experience maintaining and troubleshooting computer systems and network infrastructure.

4. I am currently assigned to investigate cyber-crime, as well as other criminal matters, and I have participated in investigations involving cyber money laundering as well as the use of computers, e-mail accounts, and the Internet. I have also participated in the execution of search warrants involving computer equipment and electronically stored information. I have received advanced training in computer investigations, interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, and various other criminal laws and procedures. Based on my training and experience, I am familiar with the means by which individuals use computers and information networks to commit various crimes.

5. I make this affidavit based upon personal knowledge derived from my training, experience, and participation in this investigation, and information that I have learned from discussions with other investigators. The facts related in this affidavit do not reflect the totality of information known to me or other officers, merely the amount needed to establish probable cause. Unless otherwise noted, wherever in this affidavit I asserted that a statement was made, the information was provided by another law enforcement officer or witness who may have had either direct or indirect or hearsay knowledge of that statement and to whom I or

others have spoken. I do not rely upon facts not set forth herein in reaching my conclusion that a complaint should be issued, nor do I request that this Court rely upon any facts not set forth herein in reviewing this affidavit.

PROBABLE CAUSE

6. The FBI, Atlanta Division, is currently investigating a cyber-money laundering network that has used unwitting U.S. citizens to cash fraudulent checks since at least May 2018 and continuing today. The funds are then transmitted back to conspirators located overseas. The FBI has obtained judicial complaints and arrest warrants issued out of the Northern District of Georgia for two other co-conspirators, IGOR ZHIRNOV (ZHIRNOV) and GRIGORII BASKAKOV (BASKAKOV), who are part of this cyber-money laundering network. Both co-conspirators are charged with violations of Title 18, United States Code, Section 1956(a)(1)(B)(i) (concealment money laundering) for their roles in work-from-home fraud schemes involving victims located in the Northern District of Georgia and elsewhere in the United States.

7. SPITSYN, like the other co-conspirators, has received and laundered proceeds from work-from-home fraud schemes, which have affected a number of victims throughout the United States.

8. ZHIRNOV, BASKAKOV and SPITSYN have been identified as individuals who has received proceeds of a number of work-from-home fraud schemes.

According to complaints filed with the FBI, the complainants were contacted by foreign companies and offered jobs that would allow them to work from home. Once hired by these foreign companies, the complainants were often asked to receive checks in the mail as part of their job and then instructed to cash the checks using their own bank account(s) and mail the cash via the United States Postal Service (USPS) to identified company “supervisors.” After completing one or more of these tasks, the complainants were later contacted by their respective banks and advised the checks they had cashed were fraudulent. The complainants were then advised by their banks that they owe the banks money as a result of cashing the fraudulent checks.

9. As part of this scheme, the FBI determined that one of the “supervisors” identified by the complainants was ZHIRNOV. Specifically, in or about May 2020, the FBI made contact with an individual, hereinafter referred to as (Victim #1), located in the Northern District of Georgia who had fallen victim to a work-from-home fraud scheme similar to what was described above. Victim #1 reported that he owed approximately \$25,000 to his¹ financial institution after he had unknowingly cashed fraudulent checks.

¹ I use “him” or “his” when referring to Victim(s) and Complainant(s) for generic purposes, which does not necessarily reflect the Victim(s) or Complainant(s) gender.

10. Victim #1 reported being directed by foreign company named “Transavia S.R.L”, hereinafter (“TRANSAVIA”), to receive a number of checks, cash the checks, and then mail the cash to identified “supervisors” provided by a representative of TRANSAVIA. Victim #1 engaged in these financial transactions within the Northern District of Georgia before speaking to the FBI about the transactions. The below table details some of the specific packages of cash Victim #1 mailed at the direction of the TRANSAVIA representative after having cashed the checks:

Mail Date	Delivery Date	Amount	“Supervisor”	USPS Tracking #
4/17/2020	4/18/2020	\$1,700	I. ZVIRNOV	EE212502654US
4/27/2020	4/28/2020	\$1,825	I. ZVIRNOV	EL744429818US
4/28/2020	4/30/2020	\$3,670	I. ZVIRNOV	EL744429804US

11. After meeting with Victim #1, the FBI reviewed email communications between Victim #1 and the TRANSAVIA representative. The communications revealed that the TRANSAVIA representative directed Victim #1 to complete the transactions shown in the above-listed table. According to Victim #1, he was contacted by his financial institution after completing a number of these transactions including the ones listed in the above-mentioned table. His financial institution advised that the checks he had cashed were fraudulent and that the bank would be holding him responsible for the amount of the cash checks, which was approximately \$24,000.

12. Additionally, communications between Victim #1 and the TRANSAVIA representative revealed that the TRANSAVIA representative provided detailed instructions for sending packages of cash to their “supervisor” I. ZVIRNOV, hereinafter (“ZVIRNOV”), which included the mailing address 1111 Wilshire Blvd #330 Los Angeles, CA 90017. Through a search warrant obtained for an email account belonging to ZHIRNOV, the FBI identified an email containing a lease agreement for the aforementioned address which listed ZHIRNOV as the resident. In addition, through legal process, the FBI determined the address was listed as a residential address for ZHIRNOV on at least one bank account.

13. As part of this scheme, the FBI determined that another one of the “supervisors” identified by the complainants was BASKAKOV. As previously described above, Victim #1 had fallen victim to a work-from-home scheme and had mailed packages of cash from the Northern District of Georgia to ZHIRNOV. In addition, the below table details additional packages of cash Victim #1 mailed at the direction of the TRANSAVIA representative after having cashed the checks:

Mail Date	Delivery Date	Amount	“Supervisor”	USPS Tracking #
5/4/2020	5/5/2020	\$1,830	GREGORII BUSKAKOV	EE212502549US
5/5/2020	5/6/2020	\$3,630	GREGORII BUSKAKOV	EL744429720US
5/11/2020	5/12/2020	\$1,780	GREGORII BUSKAKOV	EL744429530US
5/12/2020	5/13/2020	\$1,800	GREGORII BUSKAKOV	EE212502504US
5/13/2020	5/14/2020	\$1,790	GREGORII BUSKAKOV	EJ147598814US
5/14/2020	5/15/2020	\$1,800	GREGORII BUSKAKOV	EE212505911US

14. After meeting with Victim #1, the FBI reviewed email communications between Victim #1 and the TRANSAVIA representative. The communications revealed that the TRANSAVIA representative directed Victim #1 to complete the transactions shown in the above-listed table. Additionally, the communications revealed that the TRANSAVIA representative provided detailed instructions for sending packages of cash to their “supervisor” GREGORII BUSKAKOV, hereinafter (“BUSKAKOV”), which included the mailing address 138-44C Queens Blvd., #334, Jamaica, NY 11435. Through coordination with the United States Postal Inspection Service (USPIS), the FBI later determined the aforementioned address was the same address BASKAKOV registered at a UPS Store in New York. Additionally, UPS store records showed BASKAKOV picked up a number of packages at the address including some of the packages described in the above-listed table.

15. In addition to the packages in the above-listed table, BASKAKOV also received a package sent by the FBI which contained undercover funds. Specifically, using Victim #1’s email account, an undercover FBI agent in the Northern District of Georgia purported to be Victim #1 and communicated directly with the TRANSAVIA representative. During the communications, the TRANSAVIA representative directed an undercover FBI Agent acting as Victim #1 to cash additional checks and mail the cash to an individual later identified to

be BASKAKOV. Instead of cashing the checks, the FBI utilized undercover funds and mailed 2 packages of cash in May 2020. The first package was for the amount of \$1,840 and was sent to BUSKAKOV at the above-mentioned address on or about May 19, 2020. The package failed to deliver on the expected delivery date and was later returned by USPIS to the FBI. The second package contained \$1,800 and was sent to GREGOR BOSKA ("BOSKA") at the address 118-35 Queens Blvd., #400, Forest Hills, NY 11375 on or about May 21, 2020, and was delivered on May 22, 2020. Through legal process, the FBI obtained video surveillance of the aforementioned address around the time the second package was picked up and the video showed an individual matching the description of BASKAKOV retrieving approximately 8 packages including the package sent by the FBI on or about May 21, 2020.

16. In addition, the FBI received a copy of a complaint filed with the Lake Zurich Police Department in Illinois. A review of the complaint revealed an individual, hereinafter referred to as Victim #2, had fallen victim to a work-from-home fraud scheme similar to what has previously been described. According to the complaint, Victim #2 had begun working for a company named "SVILUPPO IMMO" (SVILUPPO) and was instructed to receive several checks in the mail, cash the checks, and mail the cash to identified "supervisors" of the company. Through a review of email communications included in the complaint, the FBI

determined Victim #2 was directed to send packages of cash to BOSKA at address 118-35 Queens Blvd., #400, Forest Hills, NY 11375. In addition, Victim #2 received a letter from his/her financial institution advising that at least one of the cashed checks was returned for being "Altered/Fictitious" and therefore the amount of the check would be subtracted from Victim #2's account.

Additionally, a detective from Lake Zurich Police Department provided the FBI with the below registration information she obtained regarding the aforementioned address.

Company: Gregor Boska
Name: Gregor Baskaukov
Home Address: 76 Logan Street, Cypress Hill, NY, 11208
Phone number: 781 353 1540
Email: gregoryb.russia@gmail.com

The FBI later determined that the phone number and email address provided on the above address registration belonged to BASKAKOV and was registered to at least one bank account belonging to BASKAKOV.

17. SPITSYN is a citizen of Russia who is set to arrive in the United States on August 21, 2020. SPITSYN has previously visited the United States on several occasions from 2017 to the present. The FBI also determined that another one of the "supervisors" identified by the complainants was SPITSYN. Specifically, in or about January 2019, the FBI received a complaint filed by an individual, hereinafter referred to as Complainant #1, who had fallen victim to a work-from-

home fraud scheme like what was described above. Complainant #1 reported that he² was hired by an Italian company “Investicerto”, hereinafter (“INVESTICERTO”) and directed by a representative of the company to receive a number of checks, cash the checks, and then mail the cash to identified “supervisors” provided by a representative of INVESTICERTO. Complainant #1 reported engaging in several of these types of financial transactions. The table below lists some of the transactions reported by Complainant #1:

Mail Date ³	Delivery Date ⁴	Amount	“Supervisor”	USPS Tracking #
12/18/2018	12/19/2018	\$2,490	Alex Spicyn	EE252979495
12/26/2018	12/27/2018	\$4,910	Alex Spicyn	EE252978676
12/31/2018	1/2/2019	\$4,935	Alex Spicyn	9470103699300041509826

In addition, Complainant #1 reported that the address the above packages were sent to was “331 State Street, Apt. 2F, Brooklyn, NY 11217”. Based on the aforementioned address, the FBI determined the address was listed on at least three bank statements for a Wells Fargo account ending in x5591, which belonged to SPITSYN, including statements covering December 2018 through

² I use “he” or “his” when referring to Victim(s) and Complainant(s) for generic purposes, which does not necessarily reflect the Victim(s) or Complainant(s) gender.

³ Based on the tracking numbers provided by Complainant #1, the FBI determined the package mail date.

⁴ Based on the tracking numbers provided by Complainant #1, the FBI determined the package delivery date.

January 2019. Furthermore, a review of SPITSYN'S bank account ending in x5591 revealed that he conducted cash deposits into the account on or around the same days he received some packages from Complainant #1. For example, in the table above, SPITSYN received \$2,490 from Complainant #1, which was delivered on December 19, 2018. The same day, SPITSYN conducted 4 cash deposits into his account ending in x5591 in the amounts of \$3,000, \$1,888, \$3,000, and \$2,240. The following day, December 20, 2019, SPITSYN wired \$9,901 from his account ending in x5591 to a company located overseas. Additionally, on December 27, 2018, SPITSYN received \$4,910 as reported by Complainant #1. The following day, December 28, 2018, SPITSYN deposited \$9,940 into a JP Morgan Chase Bank account ending in x9155, which was registered to himself. The same day, SPITSYN sent an international wire transfer from the account ending in x9155 to an overseas company in the amount of \$9,892.

18. In a second complaint filed with the FBI in November 2018, an individual in Nevada, hereinafter referred to as Complainant #2, reported that he had fallen victim to work-from-home scheme similar to what has previously been described. Specifically, Complainant #2 reported that he began working for an international company called "HNG Horizon", hereinafter referred to as "HNG". Complainant #2 was then directed to receive checks in the mail, cash the checks, and then mail the cash to a "supervisor" of the company. Complainant #2

completed several transactions as directed by an HNG representative, two of which included mailing \$2,597 and \$2,761 in cash to a “supervisor” named “Alex Spicyn” (SPICYN), to the address “40 Macon St #3r Brooklyn, NY 11216”.

According to Complainant #2, his bank later told him he was being scammed and that he would have to repay the bank \$5,358 for the checks he had cashed.

19. Through the investigation, the FBI determined that the address “40 Macon St #3r Brooklyn, NY 11216” was used by SPITSYN. Specifically, SPITSYN opened at least one bank account using the address and provided a copy of his passport during the opening process. In addition, SPITSYN received bank statements at the same address from accounts he opened at other financial institutions. Based on the above information, I believe SPITSYN was using the alias SPICYN to receive packages of cash at his addresses, which contained proceeds of work-from-home fraud schemes. In addition to the complaints described above, the FBI identified approximately a dozen other complaints from individuals located throughout the United States that reported similar work-from-home schemes involving SPITSYN or aliases believed to be used by him.

20. The FBI identified bank accounts for SPITSYN at several different US-based financial institutions including Bank of America, Citi Bank, JP Morgan Chase, Santander Bank, TD Bank, and Wells Fargo. A review of bank records for SPITSYN revealed large numbers of cash deposits and subsequent international

wire transfers to companies primarily located outside of the United States. For example, a Bank of America account ending in x8952 for SPITSYN revealed approximately \$250,000 in cash deposits from November 2018 through March 2019 and approximately \$250,000 in international wire transfers during the same timeframe. Additionally, a Wells Fargo account for SPITSYN ending in x5591 revealed cash deposits for approximately \$91,000 and international wire transfers for approximately \$75,000 from November 2018 through February 2019. In addition, a JP Morgan Chase account for SPITSYN revealed cash deposits for approximately \$300,000 and international wire transfers for approximately \$300,000 from December 2018 through May 2019. Furthermore, SPITSYN'S Citi Bank, Santander Bank, and TD Bank accounts revealed similar instances of cash deposits and international wire transfers. In each of the bank accounts identified for SPITSYN, the cash deposits tended to be in the amounts of \$10,000 or less. Based on my knowledge, training, and experience I know that banks are required to file Currency Transaction Reports⁵ (CTRs) for any transactions over \$10,000. Therefore, I believe SPITSYN was attempting to avoid the CTR reporting requirement by keeping his cash transactions at \$10,000 or below.

⁵ Federal law requires financial institutions to report currency (cash or coin) transactions over \$10,000 conducted by, or on behalf of, one person, as well as multiple currency transactions that aggregate to be over \$10,000 in a single day. These transactions are reported on Currency Transaction Reports (CTRs).

21. During the investigation, the FBI obtained bank account records for both SPITSYN and ZHIRNOV from a number of different US financial institutions. A review of the records revealed that SPITSYN and ZHIRNOV shared the same address on at least one occasion. Specifically, SPITSYN and ZHIRNOV both received bank account statements at the same New Jersey address during the same time period.

22. During the investigation, the FBI obtained a search warrant for the email account GRUDAKAMNEI@GMAIL.COM, which the FBI determined to belong to a co-conspirator located in Russia. A review of email communications in the account revealed numerous emails containing pictures of wire transfer documents for ZHIRNOV, BASKAKOV, and SPITSYN. For example, in an email dated on or about April 25, 2019, there was an attached picture showing a wire transfer from SPITSYN to a company located in Ecuador. Then in an email on or about May 1, 2019, an attached picture showed a wire transfer from ZHIRNOV to the same company in Ecuador. Later, in an email dated on or about July 17, 2019, the attached picture contained a copy of a wire transfer from BASKAKOV to the same company in Ecuador that ZHIRNOV and SPITSYN sent money to. Furthermore, there were numerous other emails that showed similar pictures of wire transfers from SPITSYN, ZHIRNOV, and BASKAKOV to overseas companies, including some of the same companies.

23. Based upon the foregoing, I submit there is probable cause to believe that ALEKSANDR VLADIMIROVICH SPITSYN has committed violations of Title 18, United States Code, Section 1956(h) (money laundering conspiracy).